CLAIMS

What is claimed is:

1. A method comprising:
measuring a trusted original portion of firmware;
securely storing the measurement of the trusted original portion of firmware;
measuring an unqualified current portion of firmware;
retrieving the measurement of the trusted original portion of firmware;
comparing the measurement of the trusted original portion of firmware to the measurement of the unqualified current portion of firmware; and
if the measurements match, executing the current portion of firmware as a trusted process.

2. The method of claim 1, wherein securely storing the measurement of the trusted portion of original firmware comprises storing the measurement in a trusted platform module (TPM).

3. The method of claim 2, wherein the trusted platform module is embodied as a hardware component.

4. The method of claim 2, wherein the trusted platform module is embodied as a software-based component.

5. The method of claim 1, further comprising:

enforcing a locality-based security mechanism, wherein a processor must be operating in at least one of a given locality and a higher locality to retrieve the measurement of the trusted portion of firmware.

6. The method of claim 1, wherein measuring the trusted original portion of firmware comprises measuring a startup portion of one of system management mode (SMM) firmware code and platform management interrupt (PMI) firmware code.

7. The method of claim 1, further comprising performing a core root of trust measurement (CRTM).

8. The method of claim 7, wherein the CRTM is a static CRTM comprising a measurement of a trusted bootable portion of firmware.

9. The method of claim 7, wherein the CRTM is a dynamic CRTM measured via execution of processor microcode.

10. The method of claim 1, further comprising:

creating a descriptor indicating where the trusted original portion of firmware is located.

11. A method, comprising:

measuring at least one integrity metric corresponding to a trusted portion of an original firmware configuration;

storing a respective measurement corresponding to each of said at least one integrity metric in a corresponding platform configuration register (PCR) of a trusted platform module(TPM); and

sealing a secret to the TPM, the secret contained in a digest including the secret concatenated with the respective measurement(s) stored in the PCR(s),

wherein a current firmware configuration includes a portion that matches the trusted portion of the original firmware configuration to unseal the secret.

12. The method of claim 11, further comprising:

specifying a locality to be associated with a trusted firmware process; and

concatenating the locality to the secret and the respective measurement(s) used to form the digest stored in the PCR(s).

13. The method of claim 11, further comprising:

asserting a locality corresponding to an execution privilege level;

storing at least one of the respective measurement(s) in a PCR that may be extended if a current execution privilege level matches or exceeds the locality of the execution privilege level that is asserted.

14. The method of claim 12, wherein the locality is locality 1.

15. The method of claim 11, wherein the trusted portion of the original firmware configuration includes a trusted boot block.

16. The method of claim 15, further comprising:

measuring the trusted boot block to obtain a core root of trust measurement (CRTM).

17. The method of claim 11, wherein the trusted portion of the original firmware configuration includes a startup portion of one of system management mode (SMM) firmware code and platform management interrupt (PMI) firmware code.

18. The method of claim 11, further comprising:

attempting to unseal the secret sealed to the TPM; and

executing firmware as a trusted process if the secret is unsealed, otherwise executing the firmware process as an untrusted process.

19. The method of claim 11, wherein the integrity metric is measured by executing microcode on a processor.

20. An article of manufacture, comprising:

a machine-readable medium have instructions stored thereon, which when executed perform operations including:

measuring a trusted portion of an original set of firmware components during a pre-boot phase of a computer system;

storing the measurement of the trusted portion of the original set of firmware components in a trusted platform module (TPM) platform configuration register (PCR);

measuring a portion of a current set of firmware components during an operating system (OS)-runtime phase of the computer system

determining if the measurement of the portion of the current set of firmware components matches the measurement of the portion of the original firmware components; and

providing indicia to a processor to execute the portion of the current set of firmware components as a trusted process if the measurements match.

21. The article of manufacture of claim 20, wherein each of the original and current sets of firmware components correspond to system management mode (SMM) firmware.

22. The article of manufacture of claim 20, wherein each of the original and current sets of firmware components correspond to platform management interrupt (PMI) firmware.

23. The article of manufacture of claim 20, wherein the machine-readable medium comprises further instructions to perform the operation of performing a core root of trust measurement (CRTM).

24. The article of manufacture of claim 20, wherein the machine-readable medium comprises further instructions to perform operations including:

sealing a secret to the TPM, the secret contained in a digest including the secret concatenated with the measurement of the trusted portion of the original set of firmware that is stored in the PCR.

25. The article of manufacture of claim 20, wherein the article comprises a flash device.

26. A system comprising:

a processor, including microcode instructions;

memory, operatively coupled to the processor;

a trusted platform module, operatively coupled to the processor; and

a flash device having firmware instructions stored thereon, which when executed on the processor perform operations including:

retrieving a first measurement stored in the TPM, the first measurement comprising a measurement of a trusted portion of the firmware instructions;

measuring a current portion of firmware instructions analogous to the trusted portion of the firmware instructions to obtain a second measurement;

comparing the first measurement to the second measurement; and

if the first and second measurements match, programming the microprocessor to execute the current portion of firmware instructions as a secure process.

27. The system of claim 26, wherein the microcode instructions may be executed to perform the operations of generating a dynamic core root of trust measurement (CRTM) for the system.

28. The system of claim 26, wherein the microcode instructions may be executed to perform operations including:

measuring the trusted portion of the firmware instructions to produce the first measurement; and

storing the first measurement in a platform configuration register (PCR) of the TPM.

29. The system of claim 26, wherein, wherein each of the original and current sets of firmware components correspond to system management mode (SMM) firmware.

30. The system of claim 26, wherein, wherein each of the original and current sets of firmware components correspond to platform management interrupt (PMI) firmware.